



Politica della sicurezza delle informazioni

Revisione 02 del 22.07.2024.

INDICE

1	SCOPO	2
2	DESCRIZIONE.....	2
3	AMBITO DI APPLICAZIONE	3
4	POLITICA PER LA SICUREZZA DELLE INFORMAZIONI	3
5	RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI.....	4

1 SCOPO

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti dal gruppo Adyda al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

2 DESCRIZIONE

Per Adyda la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, responsabile della loro gestione. Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, nell'ambito del campo di applicazione definito per l'ISMS, attraverso il rispetto delle seguenti proprietà:

1. **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti ed ai processi debitamente autorizzati ed analizzati tramite una attenta analisi dei rischi;
2. **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architettonici associati quando ne fanno richiesta;
4. **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità:** garantire una provenienza affidabile dell'informazione.
6. **Privacy:** garantire la protezione ed il controllo dei dati personali fin dalle fasi progettuali (Privacy by Design) con soluzioni volte alla minimizzazione nell'uso di tali dati (Privacy by default con anonimizzazione e mascheramento dei dati, dove possibile).
7. **Cybersecurity:** Adyda all'interno dei suoi processi intende garantire una attenta analisi, conoscenza e mitigazione delle vulnerabilità dei sistemi e degli applicativi al fine di implementare processi sicuri e resilienti in termini di sicurezza delle informazioni.

Nell'ambito della gestione dei servizi offerti Adyda, attraverso la propria infrastruttura tecnologica, l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione dell'ISMS, assicura:

- la garanzia di aver incaricato implementato procedure e policy che possano garantire un'alta resilienza dei servizi e di disponibilità riservatezza ed integrità delle informazioni;
- selezionare, quando necessario, partner affidabili al trattamento del proprio patrimonio informativo;
- un'elevata immagine aziendale volta alla sicurezza dei clienti;
- la completa osservanza degli accordi stabiliti con i clienti;
- la soddisfazione del cliente;
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza e di privacy

- una gestione strutturata dei cambiamenti organizzativi e tecnologici tramite progettazione, esecuzione e verifica dei cambiamenti che considerino anche i rischi previsti.

Per questo motivo Adyda ha sviluppato un sistema di gestione sicura delle informazioni seguendo i requisiti specificati della Norma ISO 27001:2022 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

3 AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni di Adyda si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito della ricezione, gestione e roll-out degli allarmi delle proprie centrali operative.

4 POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La politica della sicurezza di Adyda rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La politica della sicurezza delle informazioni di Adyda si ispira ai seguenti principi:

- a. Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
- b. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
- c. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
- d. Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza.
- e. Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
- f. Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
- g. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
- h. Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
- i. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di

procedure di sicurezza stabilite.

- j. L'organizzazione garantisce l'analisi del cambiamento climatico quale fattore di importanza per la continuità e disponibilità dei servizi presenti nel SGSI.

La politica della sicurezza delle informazioni è formalizzata nell'ISMS, viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema intranet e specifici canali di comunicazione.

5 RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

La Direzione è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni;
- processi di miglioramento continuo interni che innalzano la sicurezza delle soluzioni e dei sistemi progettati ed erogati da Adyda.